SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK HOLE PADA MANET

SKRIPSI

Oleh :

WINDY PUSPITASARI
1034010027

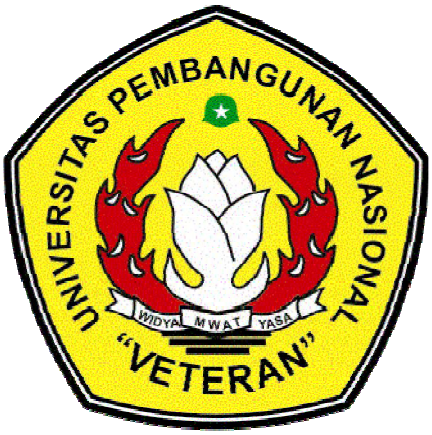
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAWA TIMUR

2014

SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK HOLE PADA MANET

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan
Dalam Memperoleh Gelar Sarjana Komputer
Jurusan Teknik Informatika



Disusun oleh :

WINDY PUSPITASARI
1034010027

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR

2014

SKRIPSI

SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK HOLE PADA MANET

Disusun Oleh :

WINDY PUSPITASARI

1034010027

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal : 23 Desember 2014

Pembimbing :

1. I Made Suartana, S.Kom, M.Kom.
   NIP. 113111984

2. Henni Endah W., ST., M.Kom.
   NPT. 3 7809 130 348 1

Tim Penguji :

1. Budi Nugroho, S.Kom, M.Kom.
   NPT. 3 8009 050 205 1

2. Barry Nugoba, S.Kom, M.Kom.
   NIP. 19841102 201212 1 002

3. Intan Yuniar Purbasari, S.Kom, M.Sc.
   NPT. 3 8006 040 1981

Mengetahui
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN FAKULTAS DEKAN TEKNOLOGI INDUSTRI UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

Ir. Sutiyono, MT
NIP. 19600713 198703 1001

LEMBAR PENGESAHAN

SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK HOLE PADA MANET

Oleh :

WINDY PUSPITASARI
1034010027

Telah disetujui mengikuti Ujian Negara Lisan
Periode Bulan Desember 2014 Tahun Akademik 2014/2015

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
I Made Suartana, S.Kom, M.Kom.	Henni Endah W., ST., M.Kom.
NIP. 113111894	NPT. 3 7809 130 348 1

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur

Budi Nugroho, S.Kom, M.Kom.
NPT. 3 8009 050 205 1

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS TEKNOLOGI INDUSTRI
PANITIA UJIAN SKRIPSI / KOMPREHENSIF
Jl. Raya Rungkut Madya Gunung Anyar Telp. (031) 8706369 (Hunting). Fax. (031) 8706372 Surabaya 60294

KETERANGAN REVISI

Mahasiswa di bawah ini :

Nama : Windy Puspitasari

NPM : 1034010027

Jurusan : Teknik Informatika

Telah mengerjakan revisi/ ~~tidak ada revisi~~*) PRA RENCANA (DESIGN) / SKRIPSI / TUGAS AKHIR Ujian lisan periode Bulan Desember 2014, TA 2014/2015 dengan judul:

"SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK HOLE PADA MANET "

Surabaya, 23 Desember 2014

Dosen Penguji yang memerintahkan revisi:

1) Budi Nugroho, S.Kom, M.Kom { }
NIP. 38090502051

2) Barry Nuqoba, S.Kom, M.Kom { }
NIP. 19841102 201212 1 002

3) Intan Yuniar Purbasari, S.Kom, M.Sc { }
NIP. 380060401981

Mengetahui,

Pembimbing Utama	Pembimbing Pendamping
I Made Suartana, S.Kom, M.Kom	Henni Endah W, S.T, M.Kom
NIP. 113111984	NPT. 378091303481

Judul : SIMULASI KINERJA MEKANISME KEAMANAN WATCHDOG ROUTING PROTOCOL AODV TERHADAP SERANGAN BLACK-HOLE PADA MANET

Pembimbing I : I Made Suartana, S.Kom, M.Kom

Pembimbing II : Henni Endah W, S.T, M.Kom

Penyusun : Windy Puspitasari

ABSTRAK

Black Hole Attack merupakan jenis serangan yang mengecoh dan menimbulkan kehilangan data berupa node berbahaya pada suatu protokol routing untuk menyebarkan informasi palsu dan mencegah paket yang terkirim. Inti dari mekanisme watchdog adalah pengawasan tepat (promiscuous monitoring). Jika terdeteksi misbehave node, source node akan memilih rute baru yang bebas dari misbehave node dengan bantuan "Path rater". Mekanisme ini tidak akan menampilkan hasil dengan baik pada saat kondisi jaringan tidak menguntungkan dimana terdapat gangguan dari misbehave node yang mengakibatkan data corrupt saat probabilitas tinggi.

Pembuktian serangan dilakukan dengan cara menjalankan file tcl melalui terminal. Source node menyebarkan route discovery process untuk membentuk jalur pengiriman menuju destination node. Bila dalam keadaan normal source node akan memilih node – node terdekat untuk membentuk suatu rute pengiriman, namun pada keadaan ini, source node tanpa disadari akan mengirimkan paket pada misbehave. Sementara untuk pembuktian mekanisme watchdog dilakukan sama persis dengan simulasi saat serangan Black Hole terjadi. Yaitu dengan memanggil program .tcl pada terminal setelah pemasangan watchdog mechanism. Perbandingan dinilai berdasarkan hasil Packet Loss selama serangan dan mekanisme berlangsung. Nilai Packet Loss saat serangan lebih besar disbanding saat mekanisme keamanan berlangsung.

Hasil perbandingan inilah yang menunjukan pengaruh dari mekanisme keamanan watchdog. Nilai packet loss saat serangan bernilai sama besarnya dengan paket terkirim yaitu 251 untuk ukuran 1000 paket sementara packet loss bernilai 1 untuk ukuran 1000 paket. Semakin kecil nilai packet loss, tingkat keberhasilan pencegahan serangan black hole dengan watchdog mechanism semakin tinggi.

Kata Kunci : Black Hole Attack, AODV, Watchdog Mechanism, NS2

KATA PENGANTAR

Puji syukur saya panjatkan kehadirat Allah SWT yang telah memberikan segala nikmat dan limpahan rahmatNya. Sehingga saya dapat menyelesaikan skripsi tepat pada waktunya dengan judul "Simulasi Kinerja Mekanisme Keamanan Watchdog Routing Protocol AODV Terhadap Serangan Black Hole Pada MANET".

Skripsi ini dibuat sebagai salah satu syarat memperoleh gelar sarjana komputer di jurusan teknik informatika UPN "Veteran" Jawa Timur. Skripsi ini dapat diselesaikan berkat bantuan dan doa dari semua pihak. Oleh karena itu, saya ingin mengucapkan terima kasih kepada :

1. Allah SWT.
2. Keluarga.
3. Bapak Prof. Dr. Ir. Teguh Soedarto, MP. selaku Rektor UPN "Veteran" Jatim.
4. Bapak Ir. Sutiyono, selaku Dekan Fakultas Teknologi Industri UPN "Veteran" Jatim.
5. Bapak Budi Nugroho, S.Kom, M.Kom, selaku Kajur Teknik Informatika.
6. Bapak I Made Suartana, S.Kom, M.Kom selaku dosen pembimbing satu.
7. Ibu Henni Endah W, S.T, M.Kom selaku dosen pembimbing dua.
8. Sahabat dan kawan – kawan seperjuangan, Echi, Nana, Ariesta, Dewi, Fara, Echa, Ade, Natalia, Mas Aris, Alpin, Cak Tri, Fian, Fiki, Dhea, Adit Mieka, Popo, Bagus, Zahry, Yudis, Alwi, Yan, Iqbal, Amik, Frans, Nyokyoto dan yang lainnya, yang tidak muat disebutkan di sini.

Saya menyadari jika skripsi ini jauh dari kesempurnaan, sehingga saran dan kritik sangat saya terima untuk menjadi lebih baik. Semoga laporan skripsi ini dapat bermanfaat khususnya bagi mahasiswa teknik informatika dan umumnya bagi orang – orang yang membutuhkan refrensi mengenai black hole attack, watchdog mechanism, routing protocol AODV dan network simulator 2.

Akhir kata, saya berharap agar penyusunan laporan ini mampu memberikan manfaat bagi perkembangan dan kemajuan teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Surabaya, 26 November 2014

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Berbagai bentuk pengembangan mengenai jaringan komputer telah banyak dilakukan. Salah satu penelitian yang dilakukan yaitu mengenai mekanisme keamanan pada suatu jaringan untuk menangkal sebuah serangan tertentu. Serangan - serangan yang ada pun terbagi dalam berbagai jenis, salah satunya adalah Black Hole Attack pada AODV dalam MANET. Black Hole Attack merupakan jenis serangan yang mengecoh dan menimbulkan kehilangan data yang berupa node berbahaya pada suatu protokol routing untuk menyebarkan informasi palsu dan mencegah paket yang terkirim. Di awali dengan menciptakan rute palsu yang dikirim kepada node source, bila berhasil maka paket yang dikirim pada node palsu ini tidak akan diteruskan ke node destination dan tidak akan dapat dilacak keberadaan paket yang telah dikirim.

Kerugian inilah yang menjadi alasan dibuatnya berbagai macam keamanan untuk mengurangi maupun manangani serangan tersebut. Salah satu bentuk keamanan yang telah diterapkan adalah mekanisme watchdog. Jenis mekanisme keamanan yang memantau dan mendeteksi malware (malicious software) yang ada pada jaringan yang diawasi. Cara kerja dari watchdog mechanism sendiri menggunakan dua pendekatan menurut Neelavathy Pari (2010), yang pertama yaitu pendekatan End to End misbehave detection menggunakan error detection coding. Dan yang kedua pendekatan yang dilakukan secara umum pada saat mengeksploitasi broadcast pergerakan - pergerakan dalam wireless medium

dimana node - node memantau arus pergerakan yang terjadi dalam satu lingkup jaringan. Tujuan dari penggunaan mekanisme keamanan watchdog ini dapat dicapai dengan melakukan pengenalan error detection coding pada watchdog mechanism, protokol yang mampu mendeteksi pergerakan misbehaving node dan pendeteksian misbehaving node pada saat probabilitas tinggi ketika throughput mencapai titik maksimal.

Hasil dari penggunaan mekanisme watchdog pada penelitian tim Kanika Lakhani (2010) menunjukan peningkatan presentase packet delivery ratio pada saat terjadi serangan dan penurunan presentase packet delivery ratio pada saat mekanisme watchdog diterapkan.

1.2 Rumusan Masalah

Adapun rumusan masalah yang akan dibahas dalam tugas akhir kali ini adalah.

a. Bagaimana melakukan simulasi serangan Black Hole pada MANET?
b. Bagaimana cara mengatasi serangan Black Hole pada routing AODV dengan mekanisme watchdog?
c. Bagaimana penerapan Black Hole attack dan watchdog mechanism pada dunia nyata?

1.3 Batasan Masalah

Agar pembahasan pada tugas akhir kali tidak mengalami perluasan dalam kajian, maka penulisan laporan ini dibatasi pada hal sebagai berikut.

a. Jumlah node yang digunakan 20 node.
b. Perbandingan yang dilakukan hanya pada saat kondisi tidak

menggunakan mekanisme keamanan dengan kondisi saat menggunakan mekanisme keamanan watchdog.

c. Serangan yang digunakan adalah Black Hole Attack. Sistem diuji secara simulasi dengan menggunakan NS2-3.5 pada OS Ubuntu 14.04
d. Penelitian hanya mencakup tentang simulasi keamanan watchdog dan simulasi serangan Black Hole.

1.4 Tujuan

Tujuan dilakukannya tugas akhir ini adalah :

a. Mengetahui bagaimana serangan Black Hole terjadi pada routing protocol AODV.
b. Mengetahui bagaimana mengamankan routing protocol AODV terhadap serangan Black Hole dengan menggunakan mekanisme keamanan watchdog.
c. Dapat mengantisipasi dan meminimalisir terjadinya serangan Black Hole.

1.5 Manfaat

Manfaat yang didapat dari penelitian ini adalah.

a. Bagi penulis mendapatkan manfaat dari pengetahuan yang diperoleh selama menempuh pendidikan di bangku perkuliahan khususnya mengenai jenis serangan Black Hole terhadap routing protocol AODV dan cara mengamankannya dengan mekanisme watchdog.
b. Bagi mahasiswa mendapatkan manfaat mengenai pemahaman akan pengamanan routing protocol AODV terhadap serangan Black Hole.

c. Bagi pembaca mendapatkan manfaat berupa informasi mengenai serangan Black Hole dan bagaimana cara mengamankannya pada routing protocol AODV untuk menjadikannya sebagai referensi tambahan serta pengembangan lebih lanjut.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini mengenai konsep dasar penyerangan Black Hole, AODV, keamanan watchdog serta MANET dan analisa yang digunakan sebagai dasar teori yang berkaitan dengan topik permasalahan yang diambil dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang metode – metode yang digunakan dalam rancangan jaringan, rancangan serangan dan rancangan keamanan pada penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil dari serangkaian konfigurasi yang telah dilakukan sebelumnya, kemudian dilakukan analisa secara menyuluruh dengan menggunakan beberapa skenario metode keamanan yang telah diterapkan.

BAB V KESIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan dari penelitian yang telah dilakukan dan saran-saran yang bermanfaat bagi peningkatan kerja sistem sebagai penutup dari Laporan Tugas Akhir ini.